National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

RedSeal Server v9.4

Report Number: CCEVS-VR-VID11104-2021
Dated: June 18, 2021
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Paul Bicknell

Linda Morrison

Clare Parran

Randy Heimann

Ted Farnsworth

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the RedSeal Server v9.4.5 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the RedSeal Server v9.4.5 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in June 2021.

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, release 5 ([1], [2], [3], [4]) and activities specified in the following document:

- Evaluation Activities for Network Device cPP, Version 2.1, September 2018 [6]

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The product is the RedSeal Server 9.4.5. It is a network device providing a Network Infrastructure Security Management (NISM) platform able to identify attack risk and non-compliance in an enterprise network. The focus of the evaluation was on the product's conformance to the security functionality specified in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 [5]

The security functions specified in this Protection Profile include protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, and ability to verify the source and integrity of updates to the TOE.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile and, when installed, configured, and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the Security Target [7]. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([12]) and the associated test report produced by the Leidos evaluation team ([11]).

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to the claimed Protection Profile and that the evaluation activities specified in [6] had been performed appropriately. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the Evaluation Technical Report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

The following table provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Evaluated Product:	RedSeal Server 9.4.5
Sponsor & Developer:	RedSeal, Inc. 1600 Technology Drive, 4th Floor San Jose, CA 95110
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	June 2021
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
Protection Profiles:	collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018
Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the TOE
Evaluation Personnel:	Greg Beaver Pascal Patin Furukh Siddique
Validation Personnel:	Paul Bicknell Linda Morrison Clare Parran Randy Heimann Ted Farnsworth

3 TOE Architecture

Note: The following architectural description is based on the description presented in the ST.

The TOE comprises the RedSeal Server application running on a Linux operating system, together with a database, all installed on a physical appliance provided by RedSeal, or provisioned as a virtual appliance image that can be deployed on a virtual platform. The scope of the evaluation covers both the hardware appliance and the virtual appliance deployed on VMware ESXi (other platforms that support the RedSeal Server virtual appliance, such as KVM, Oracle VirtualBox, and Microsoft Hyper-V, are not covered by this evaluation).

The RedSeal Server application includes the following main server processes:

- Admin server—provides administrative and infrastructure services to several other processes making up the RedSeal application
- RedSeal server—manages the import of network device configurations, contains the analysis engine, and provides the database interface.

The TOE includes a Linux distribution (CentOS 7.2-1511) that provides the operating system on which the RedSeal application executes, and Java Runtime Environment (JRE) 8, which supports part of the TOE's cryptographic algorithm implementation. The TOE (through an integrated RSA BSAFE 6.2.1) implements cryptographic algorithms that support secure communication: between the TOE and external IT entities for data collection (SSH); between the TOE and the Java client (TLS); and between the TOE and web clients (HTTPS). The TOE also includes OpenSSL 1.0.2k, which provides the cryptographic algorithms to support SSH connections to the CLI.

4 Security Policy

The TOE enforces the following security policies as described in the ST.

4.1 Security Audit

The TOE is able to generate audit records of security relevant events, including the events specified in collaborative Protection Profile for Network Devices, Version 2.1. The TOE stores audit records locally and can also be configured to send the audit records to an external syslog server over a protected communication channel.

The logs comprising the audit trail are stored in the TOE's file system and protected from unauthorized modification and deletion by file system permissions. The TOE maintains a maximum of five log files—the current log file and four backups or archives. Each file has a default maximum of 50 megabytes (which is configurable by an administrator). When the current log file reaches its configured maximum size, it is closed and rotated to an archive, and a new current log file is created. If the maximum number of archive files already exists, the oldest one is deleted. The TOE will generate a warning message if the storage space for audit records reaches 80% capacity.

4.2 Cryptographic Support

The TOE implements cryptographic algorithms and mechanisms that provide random bit generation, asymmetric cryptographic key pair generation, key establishment, symmetric data encryption and decryption, digital signature generation and verification, cryptographic hashing, and keyed-hash message authentication services in support of higher level cryptographic protocols, including SSH and TLS.

4.3 Identification and Authentication

The TOE requires all users to be successfully identified and authenticated prior to accessing its security management functions and other capabilities. The TOE offers local and remote access (via SSH) to a Command Line Interface (CLI) and remote access (protected by TLS) using the Java client to support interactive administrator sessions. There is also a browser-based Web UI available for non-administrative users to interact with the TOE.

The TOE provides a local password-based authentication mechanism for all users and enforces a minimum length for passwords. The TOE will deny remote access to a user after a configurable number of consecutive failed authentication attempts (default is three).

4.4 Security Management

The TOE provides the security management functions necessary to configure and administer its security capabilities, including: configuring a login access banner; configuring a remote session inactivity time limit before session termination; configuring the parameters (number of consecutive failures, lockout period) for the authentication failure handling mechanism; setting the system date and time and also configuring NTP; performing software updates and verifying updates using a published hash.

The TOE provides a CLI to access its security management functions. Administrators can access the CLI locally via a laptop connected directly to a network port and remotely using SSH. Additionally, some security management functions are accessible via the Java client. Security management commands are

limited to administrators and are available only after they have been successfully identified and authenticated

4.5 Protection of the TSF

The TOE protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator.

The TOE provides reliable time stamps for its own use and can be configured to synchronize its time via NTP.

The TOE provides a trusted means for determining the current running version of its software and to update its software. The integrity of software updates can be verified using a published hash.

The TOE implements various self-tests that execute during the power-on and startup sequence, including cryptographic known answer tests that verify the correct operation of the TOE's cryptographic functions.

4.6 TOE Access

The TOE will terminate local and remote interactive sessions after a configurable period of inactivity. The TOE additionally provides the capability for administrators to terminate their own interactive sessions. The TOE can be configured to display an advisory and consent warning message before establishing a user session.

4.7 Trusted Path/Channels

The TOE protects interactive communication with remote administrators using SSH (for remote access to the CLI) and remote non-administrative users using HTTPS (for access to the Web UI).

The TOE is able to protect transmission of audit records to an external audit server using TLS. It uses SSH to connect to external IT entities for the purpose of data collection, to support building its model of the network. It also protects communication with the Java client using TLS.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.
- The device is assumed to provide networking and filtering functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking/filtering functionality).
- A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP.
- The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

  For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
- The device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The administrator's credentials (private key) used to access the device are protected by the platform on which they reside.
- It is assumed that the administrator will ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in *Evaluation Activities for Network Device cPP* [6] and performed by the evaluation team).

- This evaluation covers only the specific device model and software version identified in this document, and not any earlier or later versions released or in process. Only the RedSeal Server v9.4.5 appliance (denoted G5b) and as a virtual appliance were part of the evaluation.
- The evaluation of security functionality of the product was limited to the functionality specified in the Security Target [7].
- The TOE appliances consist of software and hardware and the virtual appliance is supported on VMware ESXi v6.5.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in section 6 of this Validation Report.
- In a deployment architecture, the TOE is RedSeal Server 9.4.5. It is a network device providing a Network Infrastructure Security Management (NISM) platform able to identify attack risk and non-compliance in an enterprise network.

6 Documentation

RedSeal offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with each TOE model is as follows:

- RedSeal Installation and Administration Guide, Version 9.4 [8]
- RedSeal User Guide, Version 9.4 [9]
- RedSeal Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0 [10]

This is also provided for initial setup purposes. To use the product in the evaluated configuration, the product must be configured as specified in these guides.

Any additional customer documentation provided with the product, or which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated. Consumers are encouraged to download this CC configuration guide (CCECG above) from the NIAP website.

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary documents:

- *RedSeal Server Common Criteria Test Report and Procedures For collaborative Protection Profile for Network Devices Version 2.1* [11]

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- *Assurance Activities Report for RedSeal Networks RedSeal Server 9.4* [12]

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to *collaborative Protection Profile for Network Devices* [5].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *collaborative Protection Profile for Network Devices* [5]. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *collaborative Protection Profile for Network Devices* [5] were fulfilled.

7.1 Test Configuration

The evaluated version of the TOE consists of RedSeal Server v9.4.5 hardware appliance and a virtual appliance supported on VMware ESXi v6.5.

The TOE must be deployed as described in section 5.1 of this Validation Report and be configured in accordance with the *RedSeal Installation and Administration Guide, Version 9.4* [8], *RedSeal User Guide, Version 9.4* [9], and *RedSeal Common Criteria Evaluated Configuration Guide (CCECG),* [10].

Per Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

7.2 Vulnerability Analysis

The evaluation team performed a vulnerability analysis following the processes described in the claimed Protection Profiles and using the flaw-hypothesis methodology. This included a search of public vulnerability databases and development of Type 3 flaw hypotheses in accordance with Section A.3 of [6].

These searches were performed during the evaluation on June 9, 2021. Full results and analysis were documented in [13].

- The evaluation team searched the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search) and the https://www.redseal.net/resources/blog/ with the following keyword search terms.
- Type 1 Hypotheses (Public Vulnerability) Searches were performed on 6/9/2021 and included the following search terms:
- Router
- Switch
- TCP
- HTTPS
- SSH
- TLS
- RedSeal
- RedSeal Server
- RedSeal Client
- RedSeal vulnerability and network assessment system
- RedSeal G5b Appliance
- Broadwell E5-2637V4 – Processor
- VMware ESXi™ Hypervisor version 6.0

The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE is the RedSeal Server 9.4.5, as configured in accordance with the guidance documentation listed in Section 6 of this Validation Report.

The TOE provides an enable common criteria CLI command which must executed by an administrator to meet the claimed requirements.

8.2 Excluded Functionality

All product functionality that is not claimed by the Security Target as part of achieving exact conformance to the NDcPP is excluded from the evaluation scope.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the following documents, in conjunction with Version 3.1, Revision 5 of the CC and CEM:

- *Evaluation Activities for Network Device cPP*, Version 2.1, September 2018 [6]

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the RedSeal Common Criteria Evaluated Configuration Guide (CCECG) Version 1.0, the RedSeal Installation and Administration Guide Version 9.4 and the RedSeal User Guide Version 9.4. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The ST for this product's evaluation is *RedSeal Server v9.4 Security Target,* Version 1.0, 2021-06-18 [7].

13 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017

[5] collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018

[6] Evaluation Activities for Network Device cPP, Version 2.1, September 2018

[7] RedSeal Server v9.4 Security Target, Version 1.0, 2021-06-18

[8] RedSeal Installation and Administration Guide, Version 9.4

[9] RedSeal User Guide, Version 9.4

[10] RedSeal Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0

[11] RedSeal Server Common Criteria Test Report and Procedures For collaborative Protection Profile for Network Devices Version 2.1, Version 1.0, June 18, 2021

[12] Assurance Activities Report for RedSeal Networks RedSeal Server 9.4, Version 1.0, June 18, 2021

[13] RedSeal Server Vulnerability Assessment, Version 1.0, June 18, 2021